REMARKS/ARGUMENTS

The amendments to the specification correct a clearly typographical error. No new matter has been added by the amendments to the specification.

Claims 1-9 are pending in the present application. Claims 1-9 are amended, and claim 10 is added. Support for the new claims and claim amendments can be found in the claims as originally filed and in Applicants' patent application on page 5, paragraphs 11 and 12. Reconsideration of the claims is respectfully requested.

I. Interview Summary

Applicants thank the Examiner for the interview held on July 3, 2007 between the Applicants' representatives and the Examiner. The rejection of claim 1 under 35 U.S.C. § 103 was discussed. No agreement was reached.

II. Objections to the Claims

The Examiner objected to claims 3, 6, and 7 as containing informalities. Applicants have amended claims 3, 6, and 7 accordingly, thereby overcoming the objection.

III. 35 U.S.C. § 103, Obviousness; Claims 1-9 and New Claim 10

The Examiner rejected claims 1-9 under 35 U.S.C. § 103 as obvious over *Milo et al.*, Heuristic Profiler Software Features, U.S. Patent Application Publication 2003/0037141, February 20, 2003 (hereinafter "*Milo*") in view of *Brendel*, Method, Apparatus and Software for Network Traffic Management, U.S. Patent Application Publication 2005/0125195, June 9, 2005 (hereinafter "*Brendel*"). This rejection is respectfully traversed. With regard to claim 1, the Examiner states that:

> Regarding claim 1, *Milo* et al. show a method of detecting a denial of service attack at a network server, comprising the steps of counting the number of inbound packets and the number of discarded packets X in a specified interval (Fig.1, [0033-0040]), if the number of discarded packets X in the interval exceeds a specified minimum X(MIN) ([0040-0043]), and setting a denial of service event marker when a specified minimum is reached ([0040-00461).
>
> *Milo* et al. do not show calculating the percentage of discarded packets.
>
> *Brendel* shows calculating the percentage of discarded packets ([0023-0025, 0061-0083, 0096]).
>
> It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of *Milo* et al. with, that of *Brendel* in order to utilize a method of determining that a Denial of Service attack is occurring that considers additional information when making its determination and thus may make a more accurate determination.

Office Action dated April 5, 2007, pp. 2 and 3.

Amended claim 1, from which claims 2-10 depend, is as follows:

> 1. (Currently Amended) A method of detecting a denial of service attack at a network server, comprising:
>
> counting a number of inbound packets and a number of discarded packets in a specified interval,
>
> responsive to the number of discarded packets in the specified interval exceeding a specified minimum, calculating a percentage of discarded packets, wherein the percentage of discarded packets is the number of discarded packets divided by the number of inbound packets, and
>
> responsive to the percentage of discarded packets exceeding a specified threshold, setting a denial of service event marker.

No *prima facie* obviousness rejection can be made against amended claim 1 because neither *Milo* nor *Brendel* teach or suggest all of the claimed features of amended claim 1. Further, the proposed combination changes the principle of operation of the primary reference.

III.A. Neither *Milo* nor *Brendel* Teach or Suggest All of the Features of Claim 1

The Examiner bears the burden of establishing a *prima facie* case of obviousness based on prior art when rejecting claims under 35 U.S.C. § 103. *In re Fritch*, 972 F.2d 1260, 23 U.S.P.Q.2d 1780 (Fed. Cir. 1992). Rejections on obviousness grounds cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness. *KSR Int'l. Co. v. Teleflex, Inc.*, No. 04-1350 (U.S. Apr. 30, 2007) (citing *In re Kahn*, 441 F.3d 977, 988 (CA Fed. 2006)). Additionally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. *In re Royka*, 490 F.2d 981, 180 USPQ 580 (CCPA 1974).

A *prima facie* obviousness rejection cannot be stated because the proposed combination of the references does not teach or suggest all of the features of amended claim 1. Specifically, neither *Milo* nor *Brendel* teach or suggest (1) the feature of calculating a percentage of discarded packets, wherein the percentage of discarded packets is the number of discarded packets divided by the number of inbound packets, (2) the "responsive to" feature in the feature of responsive to the number of discarded packets in the specified interval exceeding a specified minimum, calculating a percentage of discarded packets, wherein the percentage of discarded packets is the number of discarded packets divided by the number of inbound packets, (3) the feature of responsive to the percentage of discarded packets exceeding a specified threshold, setting a denial of service event marker, and (4) the feature of counting a number of inbound packets in a specified interval.

III.A.i. Neither *Milo* nor *Brendel* Teach or Suggest the Feature of Calculating a Percentage of Discarded Packets, Wherein the Percentage of Discarded Packets is the Number of Discarded Packets Divided by the Number of Inbound Packets

Neither *Milo* nor *Brendel* teach or suggest the feature of calculating a percentage of discarded packets, wherein the percentage of discarded packets is the number of discarded packets divided by the number of inbound packets. The Examiner admits that "Milo et al. do [sic] not show calculating the percentage of discarded packets." Office Action dated April 5, 2007, p. 2. Additionally, because *Milo* is devoid of disclosure in this regard, nothing in *Milo* suggests this claimed feature.

The Examiner cites various portions of *Brendel* with respect to the calculating feature in original claim 1. Each of these portions will be addressed in turn to show *Brendel* does not teach or suggest the calculating feature in amended claim 1. The Examiner first cites the following portion of *Brendel*:

> [0023] In one aspect the invention provides a traffic evaluation device including a data interface to receive one or both of network traffic and data indicative of characteristics of network traffic and including processing means operable to evaluate the network traffic and/or data received by said data interface for predetermined characteristics that indicate that the network traffic contains a subset of attack traffic, and upon detection of said predetermined characteristics retrieve from memory information defining a superset and provide an output defining said superset, wherein the superset is a portion of the network traffic that contains said subset and defines network traffic that may be redirected and/or blocked by a network device.
>
> [0024] In another aspect the invention provides a traffic evaluation device including a data interface to receive from a network device one or both of network traffic and data indicative of characteristics of network traffic and including processing means operable to separate the network traffic and/or data indicative of characteristics of network traffic received by said network interface into a plurality of groups and evaluate each group for predetermined characteristics that indicate that the group contains a subset of attack traffic.
>
> [0025] In another aspect the invention provides apparatus for monitoring network traffic for a traffic profile abnormality, the apparatus including data volume observing means for observing the volume of data communicated to or within a network and data classification means for classifying data communicated to or within the network into one or more of a plurality of classes and a processing means operable to:
>
> > [0026] a) for at least one pair of classes compute a ratio of:
> >
> > [0027] observed data volume of one class or a function of observed data volume of one or more classes to
> >
> > [0028] observed data volume of another class or a function of observed data volume of one or more other classes;

> [0029] b) evaluate whether the one or more ratios indicate abnormal network traffic against predetermined criteria and if so output either or both of a signal indicating the potential occurrence of an attack.

Brendel, paragraphs 23-29.

Neither the cited portion nor any other portion of *Brendel* teaches or suggests the feature of calculating a percentage of discarded packets, wherein the percentage of discarded packets is the number of discarded packets divided by the number of inbound packets. *Brendel* discloses a system for preventing network traffic abnormalities, such as denial of service attacks. The cited portion also discloses defining a superset of network traffic that contains a potential subset of attack traffic so that the network traffic included in the superset may be redirected or blocked. The cited portion also discloses detecting network traffic abnormalities by analyzing ratios of different classes of network packets or traffic types. However, the cited portion does teach or suggest any classes representing the number of discarded packets or the number of inbound packets.

On the other hand, amended claim 1 recites the feature of calculating a percentage of discarded packets, wherein the percentage of discarded packets is the number of discarded packets divided by the number of inbound packets. The cited portion of *Brendel* differs from the claimed feature because the cited portion does not the teach or suggest utilizing a number of discarded packets or a number of inbound packets as operands for a calculation, let alone dividing the number of discarded packets by the number of inbound packets to obtain a percentage of discarded packets, as claimed.

For example, the cited portion states that "for at least one pair of classes," *Brendel* "compute[s] a ratio of observed data volume of one class or a function of observed data volume of one or more classes to observed data volume of another class or a function of observed data volume of one or more other classes." Even assuming, *arguendo*, that an "observed data volume" is the same as "a number," as claimed, the cited statement nowhere states that the "one or more classes" who data volume is observed relates to either inbound packets or discarded packets. Hence, the cited statement fails to disclose the operands necessary in the calculation of the percentage of discarded packets, namely, a number of discarded packets and a number of inbound packets. Therefore, neither the cited statement nor the cited portion of *Brendel* teaches or suggests the feature of calculating a percentage of discarded packets, wherein the percentage of discarded packets is the number of discarded packets divided by the number of inbound packets. As shown below, no other portion of *Brendel* teaches or suggests this claimed feature.

Next, the Examiner cites the following portion of *Brendel*:

> [0061] The apparatus 100 compares the measure of volume acquired by the processor 101 against normal levels of communication stored in the memory 103, and a database communication management functions 106 are provided in the processor 101 for this purpose. If sufficiently abnormal conditions exist (as described herein below), the apparatus 100 may issue a warning or alert, which

may be communicated by the apparatus 100 through a suitable communication interface 105. The communication interface 105 may be the same as the user interface 102 or may be a separate interface. The warning or alert may be displayed on a visual display device, an audible alarm may sound, the event may be simply logged in a log-file and/or a signal may be sent to another device for evaluation and action if required. The signal may be simply a single line going high or low, may be an email sent to a predetermined address or any other signal that communicates the warning or alert. A warning may be a passive indicator of some abnormal conditions, used to draw the attention of the system administrators to the abnormality, whereas an alarm may automatically trigger some further action, such as active filtering, as described in more detail herein.

[0062] The packets on one or more computer connections may be sampled, the sampling enforced either by the apparatus 100 or by a router or switch. The percentage of sampled packets may be 100% or less as required. Lesser percentages may be required to reduce the computational burden on the apparatus 100. The sample period and separation between samples may be configurable. Reconfiguration may be performed through the user interface 102. The configurable aspects of the apparatus 100 may be protected by a password and/or other security measures to ensure only authorised persons can reconfigure the apparatus 100.

[0063] After the apparatus 100 has observed network traffic communicated to a network, the processor 101 classifies each packet within the traffic into at least one class and increases a counter associated with that class. The classes that are made available depend on the analysis requirements for the network and may differ between networks and between sites. The apparatus 100 may be configurable to enable variation of the classes and the data packets that are included in each class. The router 110 may provide the counter values to the processor if it is able to do so. An interpreted, script-like language may be used if the processor 101 can accommodate such. Ten examples, a-j of possible classes are given below.

[0064] a. TCP packet

[0065] b. UDP packet

[0066] c. ICMP packet

[0067] d. TCP-SYN packet

[0068] e. TCP-FIN packet

[0069] f. TCP-RST packet

[0070] g. Packet longer than X bytes

[0071] h. Packet shorter than X bytes

[0072] i. Specific ICMP message type

[0073] j. Packet is IP-fragment

[0074] A single packet may fall within more than one class, in which case the counter of all classes in which it falls within may be incremented, or only selected counters may be incremented, for example based on a predefined rank.

[0075] A C-style pseudo-code example of how to implement a classification and counter for each class is given below:

```
if (new packet is received) {
        switch (IP protocol) {
        case TCP: tcp_counter++;
                break;
        case UDP: udp_counter++;
                break;
        case ICMP: icmp_counter++;
                break;
        default: other_protocol_counter++;
                break;
        }
        if (length of packet < 60) {
                short_packet_counter++;
        }
        else {
                long_packet_counter++;
        }
        ...
}
```

[0076] Those skilled in the art will recognise that modifications and improvements may be made to the classification algorithm.

[0077] The profile of network traffic communicated to the network may provide information on whether the traffic is valid. For example, the applicant believes that profile analysis is particularly advantageous for detecting denial of service attacks. Ratios can be defined between any two or more counters for the classes identified above. These ratios provide a means of establishing the traffic profile. Some examples of possible ratios, I-V are provided below.

[0078] I. Ratio of TCP packets vs. UDP packets

[0079] II. Ratio of-TCP-SYN packets vs. TCP-FIN packets

[0080] III. Ratio of short packets vs. long packets

[0081] IV. Ratio of UDP packets vs. ICMP packets

[0082] V. Ratio of IP fragments vs. non-fragmented packets

[0083] Those skilled in the art will recognise that any combination of classes may be used to define a ratio as required. The ratios may be selected to indicate the presence or absence of certain types of data in the communication monitored. The variables of a ratio need not be limited to one class, but may be a

> combination of classes. For example, two ratios may be summed, averaged or otherwise manipulated to form one variable of a ratio with another variable that may be a ratio, sum of ratios or other function of ratios. A ratio that may have particular application to web-sites is the ratio between TCP-SYN packets and the sum of TCP-FIN and TCP-RST packets. This ratio may be used to determine whether the network traffic profile is consistent with a SYN-flood attack.

Brendel, paragraphs 61-83.

Neither the cited portion nor any other portion of *Brendel* teaches or suggests the feature of calculating a percentage of discarded packets, wherein the percentage of discarded packets is the number of discarded packets divided by the number of inbound packets. Instead, the cited portion discloses grouping sampled packets of network traffic into one or more classes and defining ratios between the one or more classes to establish a traffic profile. However, the cited portion nowhere teaches or suggests that any of the one or more classes into which packets are grouped represent a number of inbound packets or a number of discarded packets, as claimed. Because the cited portion does not teach or suggest that any of the one or more classes into which packets are grouped are a number of inbound packets or a number of discarded packets, the cited portion fails to teach or suggest the operands in the division operation of amended claim 1.

For example, the cited statement lists possible classes into which packets may be grouped. These classes include: TCP packet, UDP packet, ICMP packet, TCP-SYN packet, TCP-FIN packet, TCP-RST packet, packet longer than X bytes, packet shorter than X bytes, specific ICMP message type, and packet is IP-fragment. See, *Brendel*, paragraphs 64-73. However, none of the classes listed in the cited portion are a number of inbound packets or a number of discarded packets. Instead, the listed classes relate to characteristics of a packet other than whether the packet is inbound or discarded. For example, a portion of the listed classes relate to the transmission control protocol state of a packet, such as whether the packet is a SYN, FIN, or RST packet. Therefore, the listed classes are not the same as the division operands claimed in amended claim 1, namely, a number of inbound packets or a number of discarded packets.

In another example, the cited portion discloses several possible class ratios. These ratios include: ratio of TCP packets vs. UDP packets, ratio of-TCP-SYN packets vs. TCP-FIN packets, ratio of short packets vs. long packets, ratio of UDP packets vs. ICMP packets, and ratio of IP fragments vs. non-fragmented packets. However, even assuming, *arguendo*, that the disclosed ratio is the same as a division operation, none of the classes included as part of the listed ratios are a number of inbound packets or a number of discarded packets. Because the cited portion fails to teach or suggest classes that represent a number of inbound packets or a number of discarded packets, the cited portion fails to teach or suggest the feature of calculating a percentage of discarded packets, wherein the percentage of discarded packets is the number of discarded packets divided by the number of inbound packets.

The cited portion also states that "[t]he percentage of sampled packets may be 100% or less as required." However, the cited statement discloses only the percentage of network traffic packets that are sampled for computational purposes. However, the cited statement does not teach or suggest that the percentage of sampled packets is a percentage of discarded packets, as claimed. In particular, the cited portion discloses only that the sampled packets are "packets on one or more computer connections," and fails to teach or suggest that the sampled packets relate to inbound packets or discarded packets. Therefore, neither the cited portion nor any other portion of *Brendel* teaches or suggests the feature of calculating a percentage of discarded packets, wherein the percentage of discarded packets is the number of discarded packets divided by the number of inbound packets.

Brendel's failure to teach or suggest the feature of calculating a percentage of discarded packets, wherein the percentage of discarded packets is the number of discarded packets divided by the number of inbound packets, is expected because *Brendel* does not rely on a percentage of discarded packets to prevent denial of service attacks. Instead, *Brendel* uses ratios between different network traffic classes, none of which represent a number of inbound packets or a number of discarded packets, to detect traffic abnormalities and then relies upon the analysis of those ratios to discard or redirect supersets of network traffic. Hence, *Brendel* does not teach or suggest, nor have any reason to teach or suggest, the feature of calculating a percentage of discarded packets, wherein the percentage of discarded packets is the number of discarded packets divided by the number of inbound packets.

Next, the Examiner cites the following portion of *Brendel*:

> [0096] An additional measure of whether an attack is occurring may be obtained by computing the deviation of combinations of ratios, combinations of particular values, such as a count of a particular packet type or combinations of ratios and particular values. By using such combinations, particular communication profiles can be identified that may indicate the presence of absence of a denial of service attack. This 'additional measure' of using combinations, and a da computed over the deviations of multiple statistics and/or ratios, is the most preferred method of detecting attacks, since singular statistics are usually not accurate or telling enough.

Brendel, paragraph 96.

Neither the cited portion nor any other portion of *Brendel* teaches or suggests the feature of calculating a percentage of discarded packets, wherein the percentage of discarded packets is the number of discarded packets divided by the number of inbound packets. Instead, the cited portion discloses detecting an attack based on the deviation of ratio combinations, particular values, or a combination thereof. However, the cited portion nowhere discloses that the ratios, combinations of ratios, or the particular values in any way relate to a number of discarded packets or a number of inbound packets.

For example, the cited portion states that "[a]n additional measure of whether an attack is occurring may be obtained by computing the deviation of combinations of ratios, combinations of particular values, such as a count of a particular packet type or combinations of ratios and particular values." Even assuming, *arguendo*, that the cited statement discloses a division operation, the cited statement still fails to teach or suggest that the "count of a particular packet type" relates to a number of discarded packets or a number of inbound packets. Therefore, the cited statement fails to teach or suggest the division operands recited in the claimed feature, namely, a number of discarded packets or a number of inbound packets. Therefore, neither the cited portion nor any other portion of *Brendel* teaches or suggests the feature of calculating a percentage of discarded packets, wherein the percentage of discarded packets is the number of discarded packets divided by the number of inbound packets.

As admitted by the Examiner, "*Milo* et al. do [sic] not show calculating the percentage of discarded packets." Office Action dated April 5, 2007, p. 2. Furthermore, given the absence of disclosure in *Milo* in this regard, nothing in *Milo* suggests this claimed feature. As shown above, *Brendel* does not teach or suggest this claimed feature. Therefore, the proposed combination of *Milo* and *Brendel*, when considered as a whole, does not teach or suggest all of the features of amended claim 1. For this reason, no *prima facie* obviousness rejection can be stated against amended claim 1.

III.A.ii. Neither *Milo* nor *Brendel* Teach or Suggest the "Responsive To" Feature in the Feature of Responsive to the Number of Discarded Packets in the Specified Interval Exceeding a Specified Minimum, Calculating a Percentage of Discarded Packets, Wherein the Percentage of Discarded Packets is the Number of Discarded Packets Divided by the Number of Inbound Packets

Neither the cited portion nor any other portion of *Brendel* teaches or suggests the "responsive to" feature in the feature of responsive to the number of discarded packets in the specified interval exceeding a specified minimum, calculating a percentage of discarded packets, wherein the percentage of discarded packets is the number of discarded packets divided by the number of inbound packets. As shown in Section III.A.i., neither *Milo* nor *Brendel* teach or suggest the feature of calculating a percentage of discarded packets, wherein the percentage of discarded packets is the number of discarded packets divided by the number of inbound packets. Because neither *Milo* nor *Brendel* teach or suggest the feature of calculating a percentage of discarded packets, wherein the percentage of discarded packets is the number of discarded packets divided by the number of inbound packets, *Milo* and *Brendel* cannot teach or suggest any relationship between this claimed feature and the feature of the number of discarded packets in the specified interval exceeding a specified minimum, let alone a "responsive to" relationship between the features. Therefore, neither *Milo* nor *Brendel* teach or suggest the "responsive to" feature in the

feature of responsive to the number of discarded packets in the specified interval exceeding a specified minimum, calculating a percentage of discarded packets, wherein the percentage of discarded packets is the number of discarded packets divided by the number of inbound packets.

Furthermore, even assuming, *arguendo*, that *Brendel* does teach or suggest the feature of calculating a percentage of discarded packets, wherein the percentage of discarded packets is the number of discarded packets divided by the number of inbound packets, *Brendel* still fails to teach or suggest that this claimed feature is responsive to the number of discarded packets in the specified interval exceeding a specified minimum. For example, *Brendel* provides:

> [0025] In another aspect the invention provides apparatus for monitoring network traffic for a traffic profile abnormality, the apparatus including data volume observing means for observing the volume of data communicated to or within a network and data classification means for classifying data communicated to or within the network into one or more of a plurality of classes and a processing means operable to:
>
> [0026] a) for at least one pair of classes compute a ratio of:
>
> [0027] observed data volume of one class or a function of observed data volume of one or more classes to
>
> [0028] observed data volume of another class or a function of observed data volume of one or more other classes;
>
> [0029] b) evaluate whether the one or more ratios indicate abnormal network traffic against predetermined criteria and if so output either or both of a signal indicating the potential occurrence of an attack.

Brendel, paragraphs 25-29.

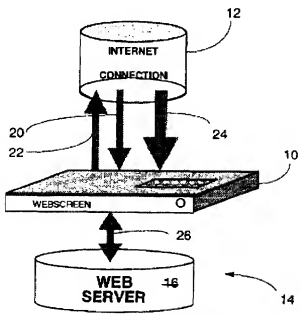
The cited portion describes a process for computing and evaluating a ratio. However, the cited portion discloses no threshold or minimum of discarded packets that must be exceeded as a condition to computing and evaluating the ratio. In addition, no other portion of *Brendel* teaches or suggests such a threshold or minimum. Therefore, even assuming, *arguendo*, that *Brendel* does teach or suggest the feature of calculating a percentage of discarded packets, wherein the percentage of discarded packets is the number of discarded packets divided by the number of inbound packets, *Brendel* still fails to teach or suggest that this claimed feature is responsive to the number of discarded packets in the specified interval exceeding a specified minimum. Accordingly, the proposed combination of *Milo* and *Brendel*, when considered as a whole, does not teach or suggest all of the features of amended claim 1.

III.A.iii. Neither *Milo* nor *Brendel* Teach or Suggest the Feature of Responsive to the Percentage of Discarded Packets Exceeding a Specified Threshold, Setting a Denial of Service Event Marker

Neither *Milo* nor *Brendel* teach or suggest the feature of responsive to the percentage of discarded packets exceeding a specified threshold, setting a denial of service event marker. Amended claim 1 defines the feature of "the percentage of discarded packets" in feature of calculating a percentage of discarded packets, wherein the percentage of discarded packets is the number of discarded packets divided by the number of inbound packets. However, as shown in Section III.A.i., neither *Milo* nor *Brendel* teach or suggest the feature of calculating a percentage of discarded packets, wherein the percentage of discarded packets is the number of discarded packets divided by the number of inbound packets. For example, the Examiner admits that "*Milo* et al. do [sic] not show calculating the percentage of discarded packets." Office Action dated April 5, 2007, p. 2. Therefore, neither *Milo* nor *Brendel* teach or suggest "the percentage of discarded packets." Because neither *Milo* nor *Brendel* teach or suggest "the percentage of discarded packets," *Milo* and *Brendel* also fail to teach or suggest the feature of responsive to the percentage of discarded packets exceeding a specified threshold, setting a denial of service event marker. Accordingly, the proposed combination of *Milo* and *Brendel*, when considered as a whole, does not teach or suggest all of the features of amended claim 1.

III.A.iv. Neither *Milo* nor *Brendel* Teach or Suggest the Feature of Counting a Number of Inbound Packets in a Specified Interval

Neither *Milo* nor *Brendel* teach or suggest the feature of counting a number of inbound packets in a specified interval. The Examiner asserts otherwise, citing the following portions of *Milo*:



[0033] Profiler 10 examines the entirety of packet traffic, both in-bound 20 and out-bound 22, as generated locally, flowing on the external network at node 12. Connection may be performed, for example, using standard Peripheral Component Interconnect (PCI) and Network Interconnect (NIC) protocols so as to operate on incoming traffic 20 without being accessible from external

sites. The profiler 10 itself has no Internet Protocol (IP) address, nor does it perform IP protocol functions such as handshakes but is, instead, transparent to ordinary data traffic between the external network and the local site. A DDoS attack, with a large volume of requests directed at local site 14, is represented in FIG. 1 by arrow 24. It is a function of profiler 10 to protect local site 14 from the effects of attack 24.

[0034] Functional operation of the profiler 10 is now described with reference to the flowchart of FIG. 2 and the database structure schematic of FIG. 3. On start-up 200, structures are created and initialized to provide the storage necessary for recording later-derived data. The database structure created on initialization includes such tables as those depicted in FIGS. 3A and 3B that are discussed in context in the following.

[0035] A program module, CheckDoRefresh 202, obtains a data packet that is inbound or outbound at the interface. (Note: program modules are named, herein, for purposes of intelligibility of the description but the functionalities associated with particularly named modules are in no way limited by virtue of the association.) Upon receipt of a packet, the profiler updates traffic statistics 204 and begins to process the Media Frame of the packet, depending upon the nature of the network involved, be it wireless, Ethernet, 802.3, Ethernet II, Frame Relay, X25, ATM, etc. In particular, the Medium Access Control (MAC) addresses of packet source and destination are checked 206 to determine whether each is internal or external to the protected site.

[0036] Furthermore, a Packet Frame processor module 208 checks for packet types. The Packet Frame processor module operates on the encapsulating frame of the packet that includes the source and destination addresses and any status flags associated with the packet. In the event that a heartbeat packet is detected, such as may be sent periodically by a server at the local site, the heartbeat packet is appropriately processed 210. If the packet is an IP packet, it is processed for successive scrutiny of IP, TCP, UDP, and ICMP syntax errors in order to detect potentially adverse traffic irregularities. Program module ProcessPacketIP 212 checks for correct IP packet syntax, and, in the case of a corrupt packet, notes the occurrence in the History Table 214 and drops the packet. Detection of anomalous packets may be logged, and, additionally, may be flagged, such as by lighting a "Bad IP" indicator such as a light. IP fragmentation analysis and fragmentation syntax checking additionally uses the IP fragment state to reject bad fragments. In this module, if an IP source identical to the IP destination is detected, the packet light is dropped and a Land attack is signaled, such as by lighting a Land attack light.

[0037] If TCP protocol is detected, program module ProcessPacketTCP 216 checks the TCP syntax of the packet, dropping it if the syntax is invalid. The history table entry corresponding to the IP source address is polled and a `charm` value is calculated. "Charm" is the subject of the following discussion.

[0038] The load on the local system 14 is constantly monitored by profiler 10, with updated activity statistics maintained in the Server Table, as shown in FIG. 3A. Load may be monitored in any of a number of ways, including the

> monitoring of data flow 26 into, and out of, the local system relative to known bandwidth limitations. Additionally, the load on the processor or processors in response to traffic 20, 22 may be monitored.
>
> [0039] Based on the load, a threshold value is set against which incoming packets will be measured, as further discussed below. The threshold measure is referred to herein as "charm." When the charm threshold has a value of zero (0), incoming packets are allowed to pass unencumbered to the local site 14. Measurement of load additionally takes into account the flow 22 of data from local site 14 to external network 12. Thus, for example, if a small number of requests results in server 16 providing a large number of pages, as may occur, for example, if the requesting source is a machine programmed maliciously to overwhelm the capacity of server 16, then the resultant load on the system is accounted for.
>
> [0040] Referring further to FIG. 2, if an incoming packet is a SYN packet, the packet-processing module 212 checks the calculated charm 218 to determine whether it exceeds the currently active charm threshold. If that is not the case, the packet is dropped after the occurrence is noted 220 for statistical purposes in the appropriate table entries. Similarly, if a valid TCP state is not detected, the packet is dropped. If more than a specified number of TCP packets are being dropped per interval of time, typically 500 TCP packets per second, a TCP flood is signaled, typically by means of a TCP flood indicator light.

Milo, paragraphs 33-40.

Neither the cited portion nor any other portion of *Milo* teaches or suggests the feature of counting a number of inbound packets in a specified interval. *Milo* discloses a system for screening packets at an interface between a local site and an external network. In particular, *Milo* screens packets by comparing incoming packets against a threshold, which *Milo* calls a "charm" value. *Milo* associates a value to candidate packets on the basis of a history table entry corresponding to the Internet Protocol source of the candidate packet. However, *Milo's* screening process does not include counting a number of inbound packets in a specified interval, as claimed.

On the other hand, amended claim 1 recites the feature of counting a number of inbound packets in a specified interval. *Milo* differs from the claimed feature because *Milo's* screening process examines each packet individually, regardless of the number of incoming packets, and *Milo's* nowhere teaches or suggests counting a number of inbound packets in a specified interval as part of the screening process.

For example, the cited portion states that "if an incoming packet is a SYN packet, the packet-processing module 212 checks the calculated charm 218 to determine whether it exceeds the currently active charm threshold." The cited statement discloses only determining whether a calculated charm for an incoming SYN packet exceeds a currently active charm threshold, but nowhere teaches or suggests counting the number of incoming SYN packets in a specified interval.

In another example, the cited portion states that "[m]easurement of load additionally takes into account the flow 22 of data from local site 14 to external network 12." The cited portion discloses only

that the "flow of data" is taken into account for load measurements. However, neither the cited portion nor any other portion of *Milo* teaches or suggests that the "measurement of load" includes counting a number of inbound packets in a specified interval.

In another example, the cited portion states that "[p]rofiler 10 examines the entirety of packet traffic, both in-bound 20 and out-bound 22, as generated locally, flowing on the external network at node 12." The cited statement discloses that the profiler examines both in-bound and out-bound packet traffic. However, the cited statement nowhere teaches or suggests that the examination of in-bound and out-bound packet traffic includes counting a number of inbound packets in a specified interval. Therefore, neither the cited portion nor any other portion of *Milo* teaches or suggests the feature of counting a number of inbound packets in a specified interval.

Brendel does not cure *Milo's* lack of disclosure. *Brendel* discloses detecting network traffic abnormalities by analyzing ratios of different classes of network packets or traffic types. However, *Brendel* nowhere teaches or suggests counting a number of inbound packets in a specified interval, and the Examiner does not assert otherwise. Therefore, the proposed combination of *Milo* and *Brendel*, when considered as a whole, does not teach or suggest all of the features of amended claim 1.

III.B. The Proposed Combination Changes the Principle of Operation of *Milo*

The Examiner has failed to state a *prima facie* obviousness rejection because the proposed combination changes the principle of operation of the primary reference. In combining references to show the claimed feature, the proposed modification cannot change the principle of operation of a reference. See *In re Ratti*, 270 F.2d 810, 123 (CCPA 1959) and MPEP 2143.01. If the proposed modification or combination of the prior art would change the principle of operation of the prior art invention being modified, then the teachings of the references are not sufficient to render the claims *prima facie* obvious. *Id.*

In the case at hand, the proposed combination of *Milo* and *Brendel* changes the principle of operation of the prior art being modified. *Milo* screens the entirely of packet traffic by comparing a charm value of each candidate packet against a threshold charm value. The calculated charm value is calculated on the basis of a history table entry corresponding to the Internet Protocol source of the candidate packet. Depending on whether the candidate packet has a sufficient calculated charm value as compared to the threshold charm value, the candidate packet will either be passed or dropped. For example, *Milo* provides:

> A computer program product and method for screening packets at an interface between a local site and an external network. A heuristic profiler scrutinizes a candidate packet and calculates a value characterizing the IP source of the packet on the basis of prior encounters with the IP source as maintained in a hashed history table entry. A filter selectively passes packets from the external

network to the site on the basis, at least, of the value ascribed to the source relative to a current threshold value determined on the basis of bandwidth usage.

....

[0018] In accordance with yet further embodiments of the invention, a method is provided for screening the flow of a candidate packet of data between an external network device and a local site. The method has the steps of:

[0019] a. identifying the external address of the candidate packet on the basis of at least the Media frame;

[0020] b. scrutinizing whether the candidate packet is malformed;

[0021] c. maintaining a hashed history table entry corresponding to each encountered IP source;

[0022] d. associating a value to the candidate packet on the basis of the history table entry corresponding to the IP source of the candidate packet;

[0023] e. selectively passing the candidate packet from the external network to the local site if the charm value associated with the candidate packet exceeds a current charm threshold; and

[0024] f. updating the current charm threshold on the basis of a bandwidth of passed packets.

....

[0033] Profiler 10 examines the entirety of packet traffic, both in-bound 20 and out-bound 22, as generated locally, flowing on the external network at node 12. Connection may be performed, for example, using standard Peripheral Component Interconnect (PCI) and Network Interconnect (NIC) protocols so as to operate on incoming traffic 20 without being accessible from external sites. The profiler 10 itself has no Internet Protocol (IP) address, nor does it perform IP protocol functions such as handshakes but is, instead, transparent to ordinary data traffic between the external network and the local site. A DDoS attack, with a large volume of requests directed at local site 14, is represented in FIG. 1 by arrow 24. It is a function of profiler 10 to protect local site 14 from the effects of attack 24.

Milo, Abstract and paragraph 33.

Thus, the entire principle of operation of *Milo's* system is to screen candidate packets by determining whether the charm value associated with the candidate packet exceeds a current charm threshold. *Milo* does not teach or suggest any other mechanism for screening the flow of data packets; indeed, to provide another mechanism for screening the flow of data packets would defeat the entire purpose of *Milo's* mechanism. Screening the flow of data packets, such as by screening invalid traffic

based on network traffic abnormalities indicated by calculated ratios of different classes of network packets or traffic types, would mean modifying, altering, or replacing the principle of operation of *Milo's* invention.

On the other hand, *Brendel* calculates ratios of different classes of network packets or traffic types and screens invalid traffic based on the presence of traffic abnormalities as indicated by the calculated ratios. For example, *Brendel* provides:

> [0025] In another aspect the invention provides apparatus for monitoring network traffic for a traffic profile abnormality, the apparatus including data volume observing means for observing the volume of data communicated to or within a network and data classification means for classifying data communicated to or within the network into one or more of a plurality of classes and a processing means operable to:
>
> [0026] a) for at least one pair of classes compute a ratio of:
>
> [0027] observed data volume of one class or a function of observed data volume of one or more classes to
>
> [0028] observed data volume of another class or a function of observed data volume of one or more other classes;
>
> [0029] b) evaluate whether the one or more ratios indicate abnormal network traffic against predetermined criteria and if so output either or both of a signal indicating the potential occurrence of an attack.
>
> [0124] If an attack is detected, for example through the ratio analysis described herein above, the apparatus 100 may start to evaluate the traffic being communicated through the router 110 and implement filters to reject invalid traffic. The processor 101 may instruct the router 110 to redirect all traffic to the processor 101 for evaluation. In some circumstances, the processor 101 may instruct the router 110 to block all traffic it receives, or implement filtering itself, or forward a group of data or another subset of traffic to the processor 101. The processor 101 may then redirect valid traffic back to the router 110 for forwarding to the corporate network 3 and discard invalid traffic. The processor 101 may therefore also act as a filter for network data.

Brendel, paragraphs 23-29 and 124 (emphasis added).

Hence, the Examiner's proposed combination changes *Milo's* principle of operation, namely, screening the flow of data packets by determining whether the charm value associated with the candidate packet exceeds a current charm threshold, because *Brendel* calculates ratios of different classes of network packets or traffic types and screens invalid traffic based on the presence of traffic abnormalities as indicated by the calculated ratios. Therefore, the teachings of *Milo* and *Brendel* fail to render amended claim 1 *prima facie* obvious.

III.C. Conclusion as to Obviousness

As shown above, no *prima facie* obviousness rejection can be made against amended claim 1. In addition, the Examiner cannot state a *prima facie* obviousness rejection against claims 2-9 and new claim 10, at least by virtue of their dependency on amended claim 1. Consequently, Applicants have overcome the obviousness rejection of claims 1-9 under 35 U.S.C. § 103.

IV. 35 U.S.C. § 103, Obviousness; Claims 1 and 2

The Examiner rejected claims 1 and 2 under 35 U.S.C. § 103 as obvious over *Milo* in view of *Levay et al.*, Apparatus and Method for Inserting Predetermined Packet Loss into a Data Flow, U.S. Patent 6,480,892, November 12, 2002 (hereinafter "*Levay*"). This rejection is respectfully traversed. With regard to claim 1, the Examiner states that:

> Regarding claim 1, *Milo* et al. show a method of detecting a denial of service attack at a network server, comprising the steps of counting the number of inbound packets and the number of discarded packets X in a specified interval (Fig.1, [0033-0040]), if the number of discarded packets X in the interval exceeds a specified minimum X(MIN) ([0040-0043]), and setting a denial of service event marker when a specified minimum is reached ([0040-00461).
>
> *Milo* et al. do not show calculating the percentage of discarded packets.
>
> *Levay* et al. show calculating the percentage of discarded packets (Fig. 7, col. 15 lines 15 - 23).
>
> It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of *Milo* et al. with that of *Levay* et al. in order to utilize a method of determining that a Denial of Service attack is occurring that considers additional information when making its determination and thus may make a more accurate determination.

Office Action dated April 5, 2007, pp. 4 and 5.

Amended claim 1, from which claim 2 depends, is as follows:

> 1. (Currently Amended) A method of detecting a denial of service attack at a network server, comprising:
>
> counting a number of inbound packets and a number of discarded packets in a specified interval,
>
> responsive to the number of discarded packets in the specified interval exceeding a specified minimum, calculating a percentage of discarded packets, wherein the percentage of discarded packets is the number of discarded packets divided by the number of inbound packets, and
>
> responsive to the percentage of discarded packets exceeding a specified threshold, setting a denial of service event marker.

No *prima facie* obviousness rejection can be made against amended claim 1 because neither *Milo* nor *Levay* teach or suggest all of the claimed features of amended claim 1. Further, no sufficient reason exists to combine *Milo* and *Levay* to achieve the invention of claim 1

IV.A. Neither *Milo* nor *Levay* Teach or Suggest All of the Features of Claim 1

A *prima facie* obviousness rejection cannot be stated because the proposed combination of the references does not teach all of the features of amended claim 1. Specifically, neither *Milo* nor *Levay* teach or suggest (1) the "responsive to" feature in the feature of responsive to the number of discarded packets in the specified interval exceeding a specified minimum, calculating a percentage of discarded packets, wherein the percentage of discarded packets is the number of discarded packets divided by the number of inbound packets, and (2) the feature of responsive to the percentage of discarded packets exceeding a specified threshold, setting a denial of service event marker.

IV.A.i. Neither *Milo* nor *Levay* Teach or Suggest the "Responsive To" Feature in the Feature of Responsive to the Number of Discarded Packets in the Specified Interval Exceeding a Specified Minimum, Calculating a Percentage of Discarded Packets, Wherein the Percentage of Discarded Packets is the Number of Discarded Packets Divided by the Number of Inbound Packets

Neither *Milo* nor *Levay* teach or suggest the "responsive to" feature in the feature of responsive to the number of discarded packets in the specified interval exceeding a specified minimum, calculating a percentage of discarded packets, wherein the percentage of discarded packets is the number of discarded packets divided by the number of inbound packets. The Examiner cites various portions of *Levay* with respect to the calculating feature in original claim 1. Each of these portions will be addressed in turn to show *Levay* does not teach or suggest the "responsive to" feature in the feature of responsive to the number of discarded packets in the specified interval exceeding a specified minimum, calculating a percentage of discarded packets, wherein the percentage of discarded packets is the number of discarded packets divided by the number of inbound packets in amended claim 1. Because the portion of *Levay* cited by the Examiner, namely column 15, lines 15-23, does not exist, Applicants assume that the Examiner meant to cite column 5, lines 15-23, which is provided below along with Figure 7:

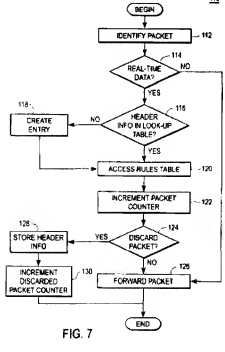


FIG. 7

> After completing a test, the stored header information and counter values can be used for analysis at a later time. In addition, statistical data can be automatically computed from the stored information. For instance, the actual percentage of total packet loss for the network under test can be computed by dividing the total number of discarded packets by the number of packets received.
>
> *Levay*, column 5, lines 15-21.

Neither the cited portion nor any other portion of *Levay* teaches or suggests the "responsive to" feature in the feature of responsive to the number of discarded packets in the specified interval exceeding a specified minimum, calculating a percentage of discarded packets, wherein the percentage of discarded packets is the number of discarded packets divided by the number of inbound packets. *Levay* discloses a test apparatus that inserts a determined amount of packet loss into a data flow so that the effects packet loss on real-time applications can be accurately measured. The cited portion discloses computing a percentage of total packet loss. However, *Levay* nowhere teaches or suggests any relationship between computing a percentage of total packet loss the number of packets discarded in a specified interval.

On the other hand, amended claim 1 recites a "responsive to" feature in the feature of responsive to the number of discarded packets in the specified interval exceeding a specified minimum, calculating a percentage of discarded packets, wherein the percentage of discarded packets is the number of discarded packets divided by the number of inbound packets. The cited portion differs from the claimed feature because the cited portion teaches or suggests no relationship, let alone a "responsive to" relationship, between computing a percentage of total packet loss and whether a number of discarded packets in a specified interval exceed a specified minimum.

For example, *Levay* states that "[a]fter completing a test, the stored header information and counter values can be used for analysis at a later time." The cited portion further states that statistical data, such as a percentage of total packet loss, may be computed from the stored data. However, the cited statement discloses only that a percentage of total packet loss may be computed "after completing a test" or "at a later time." The cited statement nowhere creates a relationship, let alone a responsive to relationship, between computing the percentage of total packet loss and a number of discarded packets in a specified interval exceeding a specified minimum. Therefore, *Levay* fails to teach or suggest the "responsive to" feature in the feature of responsive to the number of discarded packets in the specified interval exceeding a specified minimum, calculating a percentage of discarded packets, wherein the percentage of discarded packets is the number of discarded packets divided by the number of inbound packets.

Levay's failure to teach or suggest the "responsive to" feature in the feature of responsive to the number of discarded packets in the specified interval exceeding a specified minimum, calculating a percentage of discarded packets, wherein the percentage of discarded packets is the number of discarded packets divided by the number of inbound packets is expected because *Levay's* testing apparatus does not rely upon minimum specified amounts of discarded packets to execute the testing apparatus' function. Instead, *Levay* discloses varying an amount of packet loss as desired by a user to test the effects of different amounts of packet loss on real-time applications. For example, *Levay* provides that:

> The rules table is software configurable to permit a user to predictably vary the amount of packet loss occurring between the two hosts. By varying the amount of packet loss in a predetermined manner, the effect on real-time applications, such as video conferencing software, can be accurately measured.
>
> ....
>
> By altering the stored data used by the rules table, the pattern of packet loss can be varied. For example, if a ten percent packet loss is desired, the rules table can be configured such that either the first ten packets in a sequence are discarded and the next ninety are allowed to flow through the test apparatus. Alternatively, the rules table can be configured to achieve a ten percent packet loss by discarding every tenth packet in a sequence.

Levay, column 2, lines 6-11 and column 4, lines 54-61.

Because a primary purpose of *Levay's* testing apparatus is to flexibly allow the amount of packet loss to be varied, *Levay* has no reason to teach or suggest a minimum specified amount that is exceeded by the amount of packet loss. Hence, *Levay* also has no reason to teach or suggest a relationship, let alone a "responsive to" relationship, between a number of discarded packets in the specified interval exceeding a specified minimum and calculating a percentage of total packet loss. Accordingly, *Levay* fails to teach or suggest the "responsive to" feature in the feature of responsive to the number of discarded packets in the specified interval exceeding a specified minimum, calculating a percentage of discarded packets, wherein the percentage of discarded packets is the number of discarded packets divided by the number of inbound packets.

Milo does not cure *Levay's* lack of disclosure. The Examiner admits that "*Milo* et al. do [sic] not show calculating the percentage of discarded packets." Office Action dated April 5, 2007, p. 2. Furthermore, given the absence of disclosure in *Milo* in this regard, nothing in *Milo* suggests this claimed feature. As shown above, *Levay* does not teach or suggest this claimed feature. Therefore, the proposed combination of *Milo* and *Levay*, when considered as a whole, does not teach or suggest all of the features of amended claim 1. For this reason, no *prima facie* obviousness rejection can be stated against amended claim and the corresponding independent claims.

IV.A.ii. Neither *Milo* nor *Levay* Teach or Suggest the Feature of Responsive to the Percentage of Discarded Packets Exceeding a Specified Threshold, Setting a Denial of Service Event Marker

Neither *Milo* nor *Levay* teach or suggest the feature of responsive to the percentage of discarded packets exceeding a specified threshold, setting a denial of service event marker. Regarding *Milo*, the Examiner admits that "*Milo* et al. do [sic] not show calculating the percentage of discarded packets." Office Action dated April 5, 2007, p. 2. Furthermore, given the absence of disclosure in *Milo* in this regard, nothing in *Milo* suggests this claimed feature. Therefore, because *Milo* does not calculate a

percentage of discarded packets, *Milo* also does not teach or suggest the feature of responsive to the percentage of discarded packets exceeding a specified threshold, setting a denial of service event marker.

Levay does not cure *Milo's* lack of disclosure. *Levay* discloses a test apparatus that inserts a predetermined amount of packet loss into a data flow so that the effects packet loss on real-time applications can be accurately measured. However, *Levay* nowhere mentions denial of service attacks when describing the disclosed testing apparatus, let alone setting a denial of service event marker.

Therefore, the proposed combination of *Milo* and *Levay*, when considered as a whole, does not teach or suggest all of the features of amended claim 1. For this reason, no *prima facie* obviousness rejection can be stated against amended claim 1.

IV.B. The Examiner Failed to State a Sufficient Reason to Combine the References

The Examiner bears the burden of establishing a *prima facie* case of obviousness based on prior art when rejecting claims under 35 U.S.C. § 103. *In re Fritch*, 972 F.2d 1260, 23 U.S.P.Q.2d 1780 (Fed. Cir. 1992). The scope and content of the prior art are... determined; differences between the prior art and the claims at issue are... ascertained; and the level of ordinary skill in the pertinent art resolved. Against this background the obviousness or non-obviousness of the subject matter is determined. *Graham v. John Deere Co.*, 383 U.S. 1 (1966). Often, it will be necessary for a court to look to interrelated teachings of multiple patents; the effects of demands known to the design community or present in the marketplace; and the background knowledge possessed by a person having ordinary skill in the art, all in order to determine whether there was an apparent reason to combine the known elements in the fashion claimed by the patent at issue. *KSR Int'l. Co. v. Teleflex, Inc.*, No. 04-1350 (U.S. Apr. 30, 2007). Rejections on obviousness grounds cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness. *Id.* (citing *In re Kahn*, 441 F.3d 977, 988 (CA Fed. 2006)).

In the case at hand, no *prima facie* obviousness rejection can be stated because the Examiner failed to state a sufficient reason to combine *Milo* and *Levay* in light of the differences between the cited references and amended claim 1. Specifically, as shown in Section IV.A., neither *Milo* nor *Levay* teach or suggest (1) the "responsive to" feature in the feature of responsive to the number of discarded packets in the specified interval exceeding a specified minimum, calculating a percentage of discarded packets, wherein the percentage of discarded packets is the number of discarded packets divided by the number of inbound packets, and (2) the feature of responsive to the percentage of discarded packets exceeding a specified threshold, setting a denial of service event marker. Because neither *Milo* nor *Levay* teach or suggest at least these claimed features, large differences exist between the cited references and amended claim 1 under the *Graham v. John Deere Co.* inquiry set forth above.

Furthermore, the Examiner failed to state a sufficient reason to combine *Milo* and *Levay* in light of the differences that exist between the cited references and amended claim 1. The Examiner failed to state a sufficient reason to combine *Milo* and *Levay* because the Examiner's proposed reason for combining *Milo* and *Levay* provides no rational underpinning to support a legal conclusion of obviousness. Regarding a reason to combine *Milo* and *Levay*, the Examiner states that:

> It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of *Milo* et al. with that of *Levay* et al. in order to utilize a method of determining that a Denial of Service attack is occurring that considers additional information when making its determination and thus may make a more accurate determination.

Office Action dated April 5, 2007, p. 5.

However, the Examiner's proposed reason for modifying *Milo* with the teaching of *Levay*, namely, "in order to utilize a method of determining that a Denial of Service attack is occurring," provides no rational underpinning to support a legal conclusion of obviousness because *Levay* does not teach a method of determining that a denial of service attack is occurring. Instead, *Levay* discloses a test apparatus that inserts a determined amount of packet loss into a data flow so that the effects packet loss on real-time applications can be accurately measured. *Levay* nowhere mentions denial of service attacks, and nowhere discloses that the testing apparatus may be used to detect denial of service attacks. Therefore, because *Levay* does not contain the teaching that the Examiner relies upon as providing a sufficient reason for combining *Milo* and *Levay*. Therefore, the reason cited by the Examiner cannot provide a rational underpinning to support a legal conclusion of obviousness. For this reason, the Examiner's reason for combining *Milo* and *Levay* provides an insufficient basis for combining *Milo* and *Levay* in the manner proposed by the Examiner, especially in light of the large differences that exist between the cited references and amended claim 1. Accordingly, no *prima facie* obviousness rejection has been stated against amended claim 1.

IV.C. Conclusion as to Obviousness

As shown above, no *prima facie* obviousness rejection can be made against amended claim 1. In addition, the Examiner cannot state a *prima facie* obviousness rejection against claim 2, at least by virtue of the dependency of claim 2 on amended claim 1. Consequently, Applicants have overcome the obviousness rejection of claims 1 and 2 under 35 U.S.C. § 103.

V. 35 U.S.C. § 103, Obviousness; Claims 3 and 4

The Examiner rejected claims 3 and 4 under 35 U.S.C. § 103 as obvious over *Milo* in view of *Levay* and in further view of *Swander*, Method and System for Protecting a Security Parameter Negotiation Server Against Denial of Service Attacks, U.S. Patent 6,904,529, June 7, 2005 (hereinafter "*Swander*"). This rejection is respectfully traversed.

The Examiner states that:

> Regarding claim 3, *Milo* et al. in view of *Levay* et al. show the method of claim 1. *Milo* et al. in view of *Levay* et al. do not show initiating a flood monitoring process that is executed at a specified intervals to collect the relevant inbound packet information while the attack is in progress.
>
> *Swander* shows initiating a flood monitoring process that is executed at a specified interval to collect the relevant inbound packet information while the attack is in progress (col. 6 line 28 - col. 8 line 3).
>
> It would have been obvious to one of ordinary skill in the art at the time of the invention to further modify the disclosure of *Milo* et al. in view of *Levay* et al. with that of *Swander* et al. in order to continue to gather information regarding a Denial of Service attack in order to better understand the methods of the attacker and the attacks effects so that it may be better prevented andlor managed in the future.
>
> 18. Regarding claim 4, *Milo* et al. in view of *Levay* et al. and *Swander* further show resetting the denial of service event marker if the number of discarded packets in the specified interval before execution of the process is lower than a specified minimum X(MIN2), wherein X(MIN2) may or may not equal X(MIN) (*Swander*, Fig. 3 and col. 6 line 26 - col. 8 line 3).

Office Action dated April 5, 2007, pp. 5 and 6.

The rejection of claims 3 and 4 relies on the false premise that *Milo* and *Levay* can be combined in the manner the Examiner proposed *vis-à-vis* amended claim 1. As shown in Section IV.A., neither *Milo* nor *Levay* teach or suggest (1) the "responsive to" feature in the feature of responsive to the number of discarded packets in the specified interval exceeding a specified minimum, calculating a percentage of discarded packets, wherein the percentage of discarded packets is the number of discarded packets divided by the number of inbound packets, and (2) the feature of responsive to the percentage of discarded packets exceeding a specified threshold, setting a denial of service event marker. In addition, *Swander* discloses a system for protecting a network security server for negotiating network security parameters from denial of service attacks, but nowhere teaches or suggests these claimed features. Accordingly, the proposed combination of *Milo*, *Levay*, and *Swander*, when considered together as a whole, does not teach or suggest these claimed features. Therefore, the Examiner has failed to state a *prima facie* obviousness rejection against claims 3 and 4, which depend from amended claim 1.

Additionally, for the reasons presented *vis-à-vis* amended claim 1, the Examiner has failed to state a sufficient reason to combine *Milo* and *Swander* to achieve the invention of claims 3 and 4. The rejection of

claims 3 and 4 does not address the deficiencies in the rejection of claim 1. Therefore, the Examiner has failed to state a *prima facie* obviousness rejection of claims 3 and 4.

VI. Conclusion

The subject application is patentable over the cited references and should now be in condition for allowance. The Examiner is invited to call the undersigned at the below-listed telephone number if in the opinion of the Examiner such a telephone conference would expedite or aid the prosecution and examination of this application.

DATE: July 3, 2007

Respectfully submitted,

/Theodore D. Fay III/

Theodore D. Fay III
Reg. No. 48,504
Yee & Associates, P.C.
P.O. Box 802333
Dallas, TX 75380
(972) 385-8777
Attorney for Applicants

TF/ka